

EXPRESS MAIL LABEL NO.: EL863782985US

WHAT IS CLAIMED IS:

1. A method for multiplying two elements of a finite field, the method comprising the steps of:

mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree $m \cdot n$, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m ;

performing an initial KOA processing upon the two input operands in order to prepare the two input operands for multiplication in the ground field; and

performing multiplication in the ground field using a triangular basis multiplier.

EXPRESS MAIL LABEL NO.: EL863782985US

2. The method of claim 1, wherein the step of performing the initial KOA processing includes the sub-step of:

transforming an input vector including four sub-elements (a_0 , a_1 , a_2 , a_3) into an intermediate vector that is defined by:

$$\begin{pmatrix} a_0 \\ a_0 + a_1 \\ a_1 \\ a_0 + a_2 \\ \text{---} \\ a_0 + a_1 + a_2 + a_3 \\ a_1 + a_3 \\ a_2 \\ a_2 + a_3 \\ \text{---} \\ a_3 \\ x \\ x \\ x \end{pmatrix}$$

wherein the “+” operator represents a bit-wise exclusive-OR operation and “x” indicates unused or undefined values.

3. The method of claim 1, further comprising the step of performing a final KOA processing that is divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field.

4. The method of claim 1, further comprising the step of defining the first, second, and third irreducible polynomials.

5. A method for multiplying two elements of a finite field, the method comprising the steps of:

mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree $m*n$, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m ;

performing an initial KOA processing upon each of the two input operands in order to prepare the two input operands for multiplication in the ground field, the initial KOA processing being divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field; and

performing a subsequent multiplication processing upon a result of the initial KOA processing to produce a multiplicative product over the composite finite field.

6. The method of claim 5, wherein the step of performing the initial KOA processing includes the sub-step of producing a plurality of output operands that each are within the ground field.

7. The method of claim 5, further comprising the step of defining the first, second, and third irreducible polynomials.

8. A Galois field multiplier comprising:

an input operand mapper for mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree $m \cdot n$, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m ;

an initial KOA processor for performing an initial KOA processing upon the two input operands in order to prepare the two input operands for multiplication in the ground field; and

a triangular basis ground field multiplier for performing multiplication in the ground field.

9. The Galois field multiplier of claim 8,
wherein the initial KOA processor transforms an input vector including four sub-elements (a_0, a_1, a_2, a_3) into an intermediate vector defined by:

$$\begin{pmatrix} a_0 \\ a_0 + a_1 \\ a_1 \\ a_0 + a_2 \\ \text{---} \\ a_0 + a_1 + a_2 + a_3 \\ a_1 + a_3 \\ a_2 \\ a_2 + a_3 \\ \text{---} \\ a_3 \\ x \\ x \\ x \end{pmatrix}$$

wherein the “+” operator represents a bit-wise exclusive-OR operation and “x” indicates unused or undefined values.

10. The Galois field multiplier of claim 8, further comprising a final KOA processor for performing a final KOA processing that is divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field.

11. The Galois field multiplier of claim 8, wherein the first, second, and third irreducible polynomials are used-defined.

12. A finite field data multiplier for multiplying two elements of a finite field, the multiplier comprising:

an input operand mapper for mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree $m \cdot n$, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m ;

an initial KOA processor for performing an initial KOA processing upon each of the two input operands in order to prepare the two input operands for multiplication in the ground field, the initial KOA processor dividing the input operands into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field; and

a multiplier means for performing a subsequent multiplication processing upon a result from the initial KOA processor to produce a multiplicative product over the composite finite field.

13. The multiplier of claim 12, wherein the initial KOA processor produces a plurality of output operands that each are within the ground field.

14. The multiplier of claim 12, wherein the first, second, and third irreducible polynomials are used-defined.

EXPRESS MAIL LABEL NO.: EL863782985US

15. A machine-readable medium encoded with a program for multiplying two elements of a finite field, said program containing instructions for performing the steps of:

mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree $m \cdot n$, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m ;

performing an initial KOA processing upon the two input operands in order to prepare the two input operands for multiplication in the ground field; and

performing multiplication in the ground field using a triangular basis multiplier.

16. The machine-readable medium of claim 15, wherein the step of performing the initial KOA processing includes the sub-step of:

transforming an input vector including four sub-elements (a_0 , a_1 , a_2 , a_3) into an intermediate vector that is defined by:

$$\begin{pmatrix} a_0 \\ a_0 + a_1 \\ a_1 \\ a_0 + a_2 \\ \text{---} \\ a_0 + a_1 + a_2 + a_3 \\ a_1 + a_3 \\ a_2 \\ a_2 + a_3 \\ \text{---} \\ a_3 \\ x \\ x \\ x \end{pmatrix}$$

wherein the “+” operator represents a bit-wise exclusive-OR operation and “x” indicates unused or undefined values.

17. The machine-readable medium of claim 15, wherein said program further contains instructions for performing the step of performing a final KOA processing that is divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field.

18. A machine-readable medium encoded with a program for multiplying two elements of a finite field, said program containing instructions for performing the steps of:

mapping two input operands into a composite finite field that is defined by a first irreducible polynomial of degree $m \cdot n$, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m ;

performing an initial KOA processing upon each of the two input operands in order to prepare the two input operands for multiplication in the ground field, the initial KOA processing being divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field; and

performing a subsequent multiplication processing upon a result of the initial KOA processing to produce a multiplicative product over the composite finite field.

19. The machine-readable medium of claim 18, wherein the step of performing the initial KOA processing includes the sub-step of producing a plurality of output operands that each are within the ground field.

EXPRESS MAIL LABEL NO.: EL863782985US

20. A method for multiplying two elements of a finite field that is redefinable, the method comprising the steps of:

switching data bit ordering of a plurality of data bits representing a first multiplicand, such that a most significant bit of the first multiplicand is placed into a rightmost position regardless of the number of bits in the plurality of data bits representing the first multiplicand, successively less significant bits are placed into successive bits to the left of the most significant bit, and unused bits are set to zero;

converting the first multiplicand from an initial basis into a triangular basis;

switching data bit ordering of a plurality of coefficient bits representing each of a plurality of coefficients in a Galois Field generator polynomial that defines a Galois Field over which multiplication is to be performed, such that a most significant bit of each of the coefficients is placed into a rightmost position regardless of the number of bits in the plurality of coefficient bits, successively less significant bits are placed into successive bits to the left of the most significant bit, and unused bits are set to zero;

performing multiplication based upon at least the first multiplicand and a second multiplicand to produce a multiplication result; and

converting the multiplication result from triangular basis to the initial basis.

21. The method of claim 20, wherein the step of performing multiplication includes the sub-steps of:

generating a Hankel Matrix based upon the first multiplicand and the plurality of coefficients; and

multiplying the Hankel matrix with a second multiplicand to produce the multiplication result.

EXPRESS MAIL LABEL NO.: EL863782985US

22. The method of claim 20, wherein the step of switching data bit ordering of a plurality of data bits includes the step of selecting a plurality of outputs from a plurality of data multiplexers, the plurality of data multiplexers including one data multiplexer for each data bit in the plurality of data bits.

23. A machine-readable medium encoded with a program for performing the method of claim 20.

01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

EXPRESS MAIL LABEL NO.: EL863782985US

24. A flexible Galois field multiplier for multiplying two elements of a finite field that is redefinable, the multiplier comprising:

a first switching circuit for switching data bit ordering of a plurality of data bits representing a first multiplicand, the first switching circuit placing a most significant bit of the first multiplicand into a rightmost position regardless of the number of bits in the plurality of data bits representing the first multiplicand, placing successively less significant bits into successive bits to the left of the most significant bit, and setting unused bits to zero;

a first basis converter for converting the first multiplicand from an initial basis into a triangular basis;

a second switching circuit for switching data bit ordering of a plurality of coefficient bits representing each of a plurality of coefficients in a Galois Field generator polynomial that defines a Galois Field over which multiplication is to be performed, the second switching circuit placing a most significant bit of each of the coefficients into a rightmost position regardless of the number of bits in the plurality of coefficient bits, placing successively less significant bits into successive bits to the left of the most significant bit, and setting unused bits to zero;

a multiplier for performing multiplication based upon at least the first multiplicand and a second multiplicand to produce a multiplication result; and

a second basis converter for converting the multiplication result from triangular basis to the initial basis.

25. The multiplier of claim 24, wherein the multiplier generates a Hankel Matrix based upon the first multiplicand and the plurality of coefficients, and multiplies the Hankel matrix with a second multiplicand to produce the multiplication result.

EXPRESS MAIL LABEL NO.: EL863782985US

26. The multiplier of claim 24, wherein the first switching circuit includes a plurality of data multiplexers, the plurality of data multiplexers including one data multiplexer for each data bit in the plurality of data bits.

27. A modulo reduction processor for performing modulo reduction within a finite field of an unreduced data element, the finite field having a dimension equal to an integer multiple of n , the modulo reduction processor comprising:
a reduction matrix generator;
a matrix restructurer for restructuring the reduction matrix into a column vector, such that each element of the column vector is a quantity including one or more values that each are up to n bits in length; and
a reducer for reducing the data element by performing a combination of the data element and the column vector.

28. The modulo reduction processor of claim 27,
wherein the reducer includes a multiply-accumulate processing module for performing the combination of the data element and the column vector, the multiply-accumulate processing module being optimized for processing inputs of order n , and
the data element is an integer multiple of n that is greater than two.

29. The modulo reduction processor of claim 27,
wherein the reducer includes an n -bit exclusive-OR processing module for performing the combination of the data element and the column vector, and
the data element is an integer multiple of n that is greater than two.

EXPRESS MAIL LABEL NO.: EL863782985US

30. A machine-readable medium encoded with a program for performing modulo reduction within a finite field of an unreduced data element, the finite field having a dimension equal to an integer multiple of n , said program containing instructions for performing the steps of:

generating a reduction matrix;

restructuring the reduction matrix into a column vector, each element of the column vector being a quantity including one or more values that each are up to n bits in length; and

reducing the data element by performing a combination of the data element and the column vector.

31. The machine-readable medium of claim 30,

wherein in the step of reducing the data element, the combination of the data element and the column vector is performed using one or more multiply-accumulate processing modules that are optimized for processing inputs of order n , and

the data element is an integer multiple of n that is greater than two.

32. The machine-readable medium of claim 30,

wherein in the step of reducing the data element, the combination of the data element and the column vector is performed using one or more n -bit exclusive-OR processing modules, and

the data element is an integer multiple of n that is greater than two.